

SPARSE BINARY CYCLOTOMIC POLYNOMIALS

BARTŁOMIEJ BZDĘGA

ABSTRACT. We derive a lower and an upper bound for the number of binary cyclotomic polynomials Φ_m with at most $m^{1/2+\varepsilon}$ nonzero terms.

INTRODUCTION

A cyclotomic polynomial $\Phi_m \in \mathbb{Z}[x]$ is the monic polynomial of minimal degree having all the primitive m th roots of unity as its zeros. We say that the number m and the polynomial Φ_m are *binary* if m is a product of two distinct odd primes.

A. Migotti [6] proved that a binary cyclotomic polynomial Φ_m has coefficients in $\{-1, 0, 1\}$ only. The explicit number θ_m of nonzero terms of Φ_m was derived by L. Carlitz [2]. He proved that for $m = pq$ we have $\theta_m = 2p'q' - 1$, where q' denotes the inverse of q modulo p and similarly p' is the inverse of p modulo q .

It can be easily proved that for binary m we have $m^{1/2} < \theta_m < m/2$. H.W. Lenstra proved in [5] that for every $\varepsilon > 0$ there exist infinitely many binary numbers m such that $\theta_m < m^{8/13+\varepsilon}$. His method is based on the result of C. Hooley [4] that for every integer $a \neq 0$ and every $\varepsilon > 0$ there exist infinitely many primes p for which $P(p-1) > p^{5/8-\varepsilon}$, where $P(n)$ denotes the largest prime factor of n . The constant $8/13$ is presently the best possible.

The result of C. Hooley has been improved by several authors. The best result to the date is due to R.C. Baker and G. Harman [1], who proved that $P(p-1) > p^{0.677}$ for infinitely many primes p . It gives nearly 0.6 instead of $8/13$. We cannot improve the result of R.C. Baker and G. Harman, so we present a different method to achieve our goals.

We consider the set $A_\varepsilon(N)$ of integers $n < N$ for which $P(n) > n^{1-\varepsilon}$ and $P(n+1) > (n+1)^{1-\varepsilon}$. By the result of A. Hildebrand [3] the set $A_\varepsilon = A_\varepsilon(\infty)$ has a positive lower density for every $\varepsilon > 0$. We use this fact to prove the following theorem.

1991 *Mathematics Subject Classification.* 11B83, 11C08.

Key words and phrases. binary cyclotomic polynomial, nonzero terms.

Theorem. Let $B_\varepsilon(N)$ denote the set of binary $m < N$ for which $\theta_m < m^{1/2+\varepsilon}$. Then we have

$$B_\varepsilon(N) = \begin{cases} \Omega(N^{1/2}) & \text{for } 0 < \varepsilon < 1/2, \\ O(N^{1/2+\varepsilon}) & \text{for } 0 < \varepsilon < 1/6, \\ O(N/\log^2 N) & \text{for } 0 < \varepsilon < 1/2, \end{cases}$$

where we used the O and Ω asymptotical notation.

It is a well known result of Landau that

$$\#\{m \leq N : m \text{ binary}\} \sim N \log \log N / \log N.$$

From this and from the third inequality it follows that for every $\varepsilon \in (0, 1/2)$ the set $B_\varepsilon = B_\varepsilon(\infty)$ has relative density 0 in the set of binary m .

PROOF OF THE THEOREM

Part I. For every $n \in A_\varepsilon$ put $p = P(n)$, $q = P(n+1)$ and $m = pq$. Then

$$q' = \min\{a > 0 : p \mid aq - 1\} \leq (n+1)/q.$$

By the definition of A_ε we have

$$\theta_m < 2qq' \leq 2n + 2 < 2m^{1/(2-2\varepsilon)} + 2 = 2m^{1/2+\varepsilon/(2-2\varepsilon)} + 2 < m^{1/2+\varepsilon}$$

for $m > m_0$, where m_0 depends only on ε . Moreover

$$n < m^{1/2+\varepsilon} < m,$$

hence $n = pp' - 1$ or $n = qq' - 1$. If both of them are in A_ε , then

$$2m^{1/2+\varepsilon} > (pp' - 1) + (qq' - 1) = m - 1.$$

So for $m > m_1$ (where m_1 also depends only on ε) we can determine n uniquely by m . We have $m > n$, thus every $n > m_1$ is determined uniquely by m .

Let $M = \max\{m_0, m_1\}$. By the inequality

$$m \leq n(n+1)/2 < n^2$$

the function

$$f : A_\varepsilon(N^{1/2}) \setminus [1, M] \rightarrow B_\varepsilon(N), \quad f(n) = P(n)P(n+1)$$

is injective and so

$$\#B_\varepsilon(N) = \Omega(\#A_\varepsilon(N^{1/2})) = \Omega(N^{1/2})$$

by the result of A. Hildebrand mentioned in the introduction.

Part II. For $m = pq \in B_\varepsilon$ put $n = \min\{pp', qq'\} - 1$. The following facts

$$pp' + qq' = m + 1, \quad (pp')(qq') < (m+1)m^{1/2+\varepsilon}$$

imply that $n < Cm^{1/2+\varepsilon}$ for some constant C depending only on ε . Also

$$m^{1/2+\varepsilon} > \theta_m = 2p'q' - 1 > p, q,$$

thus $p, q > m^{1/2-\varepsilon}$. We have $p \mid n$ and $q \mid n+1$ (or inversely). Moreover

$$\frac{\log n}{\log \min\{p, q\}} \leq \frac{\log C + (1/2 + \varepsilon) \log m}{(1/2 - \varepsilon) \log m} = \frac{1/2 + \varepsilon}{1/2 - \varepsilon} + o(1).$$

Thus $p = P(n)$, $q = P(n+1)$ (or inversely) for m large enough, because $(1/2 + \varepsilon)/(1/2 - \varepsilon) < 2$ for $\varepsilon < 1/6$. We define m_2 to be the smallest number satisfying the following condition:

$$\text{if } m > m_2 \text{ then } m = P(n)P(n+1).$$

It is obvious that m_2 depends only on ε . Thus the function

$$g : B_\varepsilon(N) \setminus [1, m_2] \rightarrow A_\varepsilon(CN^{1/2+\varepsilon}), \quad g(pq) = \min\{pp', qq'\} - 1$$

is an injection. Finally

$$\#B_\varepsilon(N) = O(\#A_\varepsilon(CN^{1/2+\varepsilon})) = O(N^{1/2+\varepsilon})$$

due to the result of A. Hildebrand.

Part III. We assume that $m = pq$ with $q > p$. By the inequality $\theta_m > q$, if $\theta_m < m^{1/2+\varepsilon}$ then $q < p^{(1/2+\varepsilon)/(1/2-\varepsilon)}$. Thus

$$\begin{aligned} B_\varepsilon(N) &= O \left(\sum_{p < N^{1/2-\varepsilon}} \left(\pi(p^{(1/2+\varepsilon)/(1/2-\varepsilon)}) - \pi(p) \right) \right. \\ &\quad \left. + \sum_{N^{1/2-\varepsilon} < p < N^{1/2}} \left(\pi(N^{1/2}) - \pi(p) \right) \right) \\ &= O \left(\pi(N^{1/2-\varepsilon})\pi(N^{1/2+\varepsilon}) + \pi(N^{1/2})^2 \right) = O(N/\log^2 N), \end{aligned}$$

which completes the proof. \square

ACKNOWLEDGMENTS

The author would like to thank Maciej Radziejewski for helpful discussion and Pieter Moree for his remarks.

REFERENCES

- [1] R.C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), 331–361.
- [2] L. Carlitz, *The number of terms in the cyclotomic polynomial $F_{pq}(x)$* , Amer. Math. Monthly **73** (1966), 979–981.
- [3] A. Hildebrand, *On a conjecture of Balog*, Proc. Amer. Math. Soc. **95** (1985), 517–523.
- [4] C. Hooley, *On the largest prime factor of $p + a$* , Mathematica **20** (1973), 135–143.
- [5] H.W. Lenstra, *Vanishing sums of roots of unity*, Proceedings, Bicentennial Congress Wiskundig Genootschap, Vrije Univ., Amsterdam (1978), Part II (1979), 249–268.
- [6] A. Migotti, *Aur Theorie der Kreisteilungsgleichung*, Z. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien, **87** (1883), 7–14.

STRÓŻYŃSKIEGO 15A/20, 60-688 POZNAŃ, POLAND
E-mail address: exul@wp.pl